Qualys CMDB Sync App
User Guide

January 11, 2019
# Table of Contents

Preface ................................................................................................................................. 4  
  About Qualys ..................................................................................................................... 4  
  Qualys Support .................................................................................................................. 4  

Introduction to Qualys CMDB App ...................................................................................... 5  
  Prerequisites ..................................................................................................................... 5  
  Setup .................................................................................................................................. 6  

Schedules .............................................................................................................................. 7  
  ServiceNow user's Timezone setting.................................................................................. 7  
  Qualys to ServiceNow Scheduling .................................................................................. 7  
  ServiceNow to Qualys Scheduling .................................................................................... 8  
  Properties .......................................................................................................................... 9  

Sync .................................................................................................................................... 10  
  Import Queue .................................................................................................................... 10  
  Approve Qualys Assets ..................................................................................................... 10  

Export Queue ....................................................................................................................... 12  
  App Scheduled Jobs ......................................................................................................... 12  
  Transform Maps ............................................................................................................... 13  
  Reports ............................................................................................................................... 13  
  Qualys Assets Tags by Source ......................................................................................... 14  
  Assets Tag Distribution .................................................................................................... 14  
  OS Distribution ............................................................................................................... 15  

Debugging and Troubleshooting .......................................................................................... 16  

Common Questions .............................................................................................................. 17  
  Qualys to ServiceNow Sync ............................................................................................. 17  
  ServiceNow to Qualys Sync .............................................................................................. 17  

---

Qualys CMDB Sync App
Preface

Welcome to Qualys Cloud Platform! In this guide, we’ll show you how to use the Qualys CMDB Sync App to synchronize Qualys IT asset discovery and classification with the ServiceNow Configuration Management Database (CMDB) system.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/
Introduction to Qualys CMDB App

The Qualys CMDB Sync App synchronizes Qualys IT asset discovery and classification with the ServiceNow Configuration Management Database (CMDB) system. The App automatically updates the ServiceNow CMDB with any assets discovered by Qualys and with up-to-date information on existing assets, giving ServiceNow users full visibility of their global IT assets on a continuous basis. Conversely, if an asset is added to the ServiceNow CMDB, the App will add it to the Qualys asset inventory. For assets that exist in both asset repositories, selected metadata can be synchronized.

To know about the latest versions of SNOW supported, visit the CMDB Sync listing in the ServcieNow Store.

Upgrade to 1.2.0
Version 1.2.0 onwards, we have updated choice lists for “Qualys API truncation limit” and “Import batch size” properties.

Before you initiate the upgrade to 1.2.0, to get the updated choice lists, follow the steps given in the document: https://docs.servicenow.com/bundle/kingston-application-development/page/build/system-update-sets/task/t_OverwriteCustomizesDuringUpgrades.html

Prerequisites
Make sure you have a valid Qualys Account Subscription with API Access.

Visit the ServiceNow Store, search for this app, and click Contact Seller. Your TAM will be in touch regarding pricing, and then ServiceNow will provision the app into an instance of your choice. After that, the app will start appearing in the “Downloads” list in your instance. Then you need to click the “Install” button there to start using the app. After you are done, you will have a new module in your ServiceNow instance that looks like this:
Setup

After installation, add API source(s). Go to Qualys CMDB Sync App > Configuration > API Sources, and click New. Enter required details in the form.

Name is anything you would like to call it, and Username and Password are valid Qualys Cloud Platform credentials with API access enabled.

1) After you fill in the required fields, click Submit to save the API source.

2) After configuring and saving the API source, choose the connection you just built, and click Test Connection. Once you have a successful connection you are ready to move on to Schedules.
Schedules

You will need to setup at least 1 schedule. You may eventually want many more.

ServiceNow user’s Timezone setting

In the schedule scripts we use ServiceNow’s new GlideDateTime().getDisplayValueInternal() function to update the schedule last_run_timestamp. When this object is instantiated directly and used (e.g. in scoped application background script), it returns time in GMT, irrespective of the timezone set for user under whom this script runs. That’s how it is designed. Also, since Service Now does not allow scoped applications to set the timezone, app cannot do that on behalf of the user who created the schedule. BUT, the time value you see on the UI is shown in the user set timezone - even if you set GMT date-time in this column. When the schedule runs next time, it gets value in GMT, and not the one you see on UI. That may lead to confusion, and log entries show time in GMT, for this reason we recommend that the Service Now user set his or her time to GMT.

Qualys to ServiceNow Scheduling

You will give this configuration a Name, choose the API Source you setup in the previous step, and a Qualys Asset Tag you want synced over. We do not recommend leaving this blank. Also, choose if you would like us to sync Ports, Software and Hardware information. The more detailed a scan you have done with Qualys Cloud Platform, the more detail you will have here. The Cloud Agent will have the most detail of an asset, while Authenticated Scans will have the next most detail, with Un-authenticated scans having the least.

From version 1.2.1, the app has time restrictions on transaction run time. Although by default the time restriction is set to 10 minutes, you can change the time restriction to any time between 10 and 60 minutes by configuring Max Transaction Lifetime (in minutes): on Properties page. If you configure the transaction time to 20 minutes, the transaction is stopped after 20 minutes. In such a case, next scheduled run will resume from where the earlier run was stopped.

For initial sync from Qualys to ServiceNow, we recommend that you plan your schedules at an interval of every fifteen minutes.
ServiceNow to Qualys Scheduling

It is mandatory for you to either choose a Qualys Asset Tag or Qualys Asset Group. The “Qualys Asset Tag” or “Qualys Asset Group” box will assign that tag in Qualys Cloud Platform to any assets synced from ServiceNow.

Note - The Asset Tags and Asset Groups that belong to only Network_range type are populated. All other asset tags and asset groups are ignored.

We also highly recommend you add filter conditions (at minimum IP Address) to assets to be synced. When you select a TABLE ensure that the table has a column with “ip_address” name, else the ServiceNow > Qualys sync may not function. Finally you must enable VM (Vulnerability Management) to be able to scan the assets you sync. It is optional to enable PC (Policy Compliance).

What’s New

From version 1.2.1, a new option allows you to choose a tracking method when syncing from ServiceNow to Qualys. Choose IP, DNS, or NETBIOS tracking method.
You may define application specific properties on this page. The properties are self-explanatory.

1) Select the Qualys Import API call truncation limit. This property defines how many host assets to include in a single Qualys API response.

For host asset APIs, default truncation limit is 100 - i.e. if you do not provide that in preferences, it will return 100 records. However, you can provide any value between 1-100. If you provide truncation limit which is greater than 100, it results in INVALID_REQUEST error.

In our SN app, we have set the default value to 100. If SN is killing the import queue processing jobs, then user can lower that value so that XML processing time fits in job execution time limits.

We have provision to up that truncation limit up to 100, in case customer knows their assets do not have much data (ultimately resulting in smaller XML size) and if they want to keep number of API calls made as low as possible.

For example, you can set higher truncation limit if you aren’t pulling any hardware/software information. In such a case, each host asset record will not have huge information associated. One should use that only if they KNOW that information in each record will be smaller.

2) Size of Import batch is now restricted to 1
3) Select Size of Export batch
4) Allow Asset Group Sync
5) API Timeout Setting (in milliseconds)
6) Max Transaction Lifetime (in minutes)
7) Enable Debug logs?
Sync

Import Queue

This shows the list of jobs run from Qualys TO ServiceNow Assets. The status indicates whether application was able to parse the XML response successfully. The XML that was transferred is also available here (usually attached as response.xml):

Approve Qualys Assets

Assets imported from Qualys to Service Now will be here for approval after successful processing in Import Queue. If processing fails for any record in import queue (status = Error), none of the host assets in that XML will be visible here. You will need to approve each individually or a screen at a time. It will overwrite data in your CMDB if you approve the asset.
If fields gathered aren’t showing in your list, do the following:

1) Referring the same screen shot, click on the gear icon that’s to the upper left of main pane.

2) In the pop up that opens, you see two lists - Available and Selected.

3) Find and double-click “MAC Address” from the Available list. It will end up in Selected list.

4) Click OK.

Now your view refreshes, and you should start seeing the MAC address column. We set values when that tag is present in XML. So, if for some interfaces MAC address is not available (XML does not contain it OR it’s empty), the value in SN table column would be empty. It’s the same reason why you don’t see Hostname for all the network interfaces in the sample.
Export Queue

This is the list of assets to be synced from ServiceNow to Qualys Cloud Platform. If an IP Address exists in Qualys Cloud Platform we do not overwrite, we skip it and move on. Once the app successfully syncs the asset (successfully adds the IP address to user subscription), corresponding record from this list is removed. In case of any error, the record is retained with Error state, and “processing notes” column reflects some information about error.

App Scheduled Jobs

All of the Apps schedules jobs are listed under Advanced > App Scheduled Jobs. An important one to be aware of is the “Qualys Asset Tags fetching job” which runs daily by default. This syncs all of the Asset Tags in Qualys Cloud Platform for use within the App. You may wish to run this more than once a day if you generate tags in Qualys Cloud Platform on a more regular basis.
Transform Maps

A transform map is a set of field maps that determine the relationships between fields in an import set and fields in an existing ServiceNow table, such as Incidents [incident] or Users [sys_user]. After creating a transform map, you can reuse it to map data from another import set to the same ServiceNow table. The Transform Maps module enables an administrator to define destinations for imported data on any ServiceNow table. Transform mapping can be as simple as a drag and drop operation to specify linking between source fields on an import set table and destination fields on any ServiceNow table. Use transform mapping to map source and destination fields dynamically. The Transform Maps that the Qualys CMDB Sync App uses are now all listed in a handy location here.

Learn more on Transform Maps:

Reports

We give you a few canned reports as an example of the kind of data visualization you can do with ServiceNow and the Qualys App for ServiceNow data.
Qualys Assets Tags by Source

Assets Tag Distribution
OS Distribution

The image shows a pie chart displaying the distribution of operating systems. The chart indicates that Windows 10 Enterprise is the most common, followed by other operating systems with varying percentages.

Key points:
- Windows 10 Enterprise: 31.33%
- Ubuntu / Linux: 16.07%
- Other: 52.60%


Debugging and Troubleshooting

How to debug
1) Application writes log entries at appropriate places, and after each important step.
2) Also, whenever application finishes important activity, it logs “<activity> Completed” entries.
3) In case of problems, search the Application Logs module to find all the entries related to this application. See what all messages are logged by application, related to problem area.
4) If application’s log entries are not sufficient enough, and if you have access to script includes, you may add your own log statements.

Observed Issues, how to troubleshoot them and work-arounds
1) In case of huge data returned by Qualys API, the Import Queue Processor may timeout and terminate. In such a case, go to Properties page and lower the Import API call truncation limit. Additionally, the user will also need to go to the corresponding schedule, and empty the “Last run timestamp” field.
2) Issue with ServiceNow GlideSysAttachment.getContent():
   - If attachment size is more than 5mb, the getContent() method returns an empty string (“"”), even though attachment in Import Queue record shows correct and complete XML.
   - In such a case, application puts that import queue entry in “Error” state, and updates the “processing_notes” column with “Cannot process the attachment. File size maybe too large.”
   - If you encounter such a situation, you are advised to lower the “x_qual5_cmdb_sync.import_truncation_limit” property value to such a number, where response size will be under 5mb.

Anticipated Issues
1) No connection to API server. Such a case should get handled in Qualys Assets Sync script include, leading to graceful exit with proper log entries.
2) Import Queue Processor timeout during processing a particular response. This may leave the corresponding Import Queue entry in “Processing” state for quite a long time. In such a case, user should manually change the status back to
   - “Queued”, if he wants to process that response again. If you reprocess any response, it will not lead to duplicate data, as application checks whether the record already exists in staging tables before inserting.
   - ”Error”, if he does not want to process it again.

List of expected failure modes
- Qualys API server down
- Qualys subscription expired
- User credentials used are incorrect
- User credentials are correct, but they do not have API access
Common Questions

Qualys to ServiceNow Sync

Do you currently or do you plan to support the IndentifyAndReconcile API for CMDB CRUD actions?

https://docs.servicenow.com/product/configuration_management/concept/c_CMDBIdentifyandReconcile.html The goal of this API is to maintain the integrity of the database, and to correctly identify CIs so that new records are created only if CI is truly new to CMDB. The current version does not support this API. And, as of now, there is no plan to use it. However, we use transform maps and coalesce feature to update the matching record, if found. (matched on IP address only) If no matching record is found, only then will it create a new one.

Is the comparison delta derived from just a few tables or the base CMDB_CI table?
The records are primarily compared and updated/created on cmdb_ci_computer table. However, if the user wants to use any other table, they can easily update the transform map to work with the table of their choice.

Do you re-class the CI record if your IP endpoint device changes? Do you have a list of classes you have mapped for CI record creation?

We do not alter the class of CI record.

When you create/update a CI record do you record a datetime and identifier somewhere other than the description field for proper sorting/filtering?

Whenever the record in cmdb_ci_computer table is updated/newly created, we set “discovery_source” column to “Qualys”. If you search with “Discovery source contains Qualys”, you should get all these records.

What fields in SN do ports, software and hardware write to if checked?

Since there are no out-of-box tables in ServiceNow serving our purpose to store this information, we have added new tables in the application scope. Except network adapters and volumes, rest of the information (open ports, installed software, processors) go into these tables in app scope. Network adapters information goes into cmdb_ci_network_adapter table and volumes information goes into cmdb_ci_file_system table.

ServiceNow to Qualys Sync

Is it possible to sync back more than one table?

Yes, you need to create one schedule per table.